UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/451,090	11/30/1999	RAVI SANDHU	GMU-16U	8582

28598 7590 04/06/2005

GEORGE MASON UNIVERSITY
OFFICE OF TECHNOLOGY TRANSFER, MSN 5G5
4400 UNIVERSITY DRIVE
FAIRFAX, VA 22030

EXAMINER	
DINH, KHANH Q	

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 04/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/451,090	SANDHU ET AL.	
	Examiner	Art Unit	
	Khanh Dinh	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *79,80,82-90,92-95 and 97-121* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *79, 80, 82-90, 92-95 and 97-121* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the Amendment filed on 9/13/2004. Claims 79, 80, 82-90, 92-95 and 97-117 and new claims 118-121 are presented for examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patent ability shall not be negative by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 79-82, 97-100, 112, 113, 115-121 are rejected under 35 U.S.C. 103(e) as being unpatentable over Kirsch, US pat. No.5,963,915 in view of Gupta et al., US pat. No.6,226,752.

As to claim 79, Kirsch discloses a system for transfer of secure data on a network (internet 14 fig.1) comprising:

a) a client (12 fig.1) capable of presenting conforming client data.

b) a server (server 16 fig.1) capable of using said conforming client data to create at least one secure cookie (i.e., using the server to create and to store a client side cookie for use in connection with a subsequent URL request , see figs.1, 2, abstract, col.5 line 53 to col.6 line 49 and col.7 line 43 to col.8 line 52), at least one secure cookie including:

i) a domain field capable of holding domain data to associate said secure cookie to a domain where said secure cookie is valid (i.e., cookie having a match of domain, see fig.3, col.11 lines 15-38).

ii) at least one name field capable of holding name data (see col.11 lines 15-38).

iii) at least one value field capable of holding value data derived from said conforming client data (see col.11 line 39 to col.12 line 16).

iv) an expiration field capable of holding cookie expiration data (expiration date, col.13 lines 15-67).

c) a network (processing information over a network) capable of transporting at least one secure cookie between said server and said client (see fig.4, 14 lines 1-43).

d) a client storage (cookies stored by client) means capable of storing at least one of said at least one secure cookie and a secure attribute service between said client and said server using said at least one secure cookie (see col.13 line 15 to col.14 line 65).

Kirsch does not specifically disclose another cookie in the secure data processing. However, Gupta discloses a cookie containing an encrypt session key capable of encrypting said vale data contained in another of at least one secure cookie (cookie that can that encrypt/decrypt a message, see col.12 lines 7-61 and col.13 line 41 to col.14 line 45). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Gupta's teachings into the computer system of Kirsch to process secure data information because it would have enabled servers to authenticate/process users by implementing users' cookies or tokens in a communications network.

As to claim 80, Kirsch discloses a web browser (Client browser) (see col.6 lines 3-49).

As to claim 82, Kirsch discloses the secure attribute service including said server authenticating said client by comparing said conforming client data to said value data

(i.e., processing data upon receiving a URL request from a client and creating a cookie according to a user, see fig.2, col.7 line 20 to col.8 line 43).

As to claims 112 and 115, Kirsch further discloses creating integrity data from at least one secure cookie, encrypting client data (using encrypting mechanism, see col.13 lines 15-67), inputting integrity data into a seal cookie and storing said cookie (see col.14 lines 1-65).

As to claim 97, 98 and 116, Kirsch discloses that at least one of said at least one secure cookie is used in an electronic transaction and a part of a role based access control system and at least one of said at least one secure cookie is used in assigning client roles (verifying a valid user account, col.8 lines 13-63 and col.13 lines 15-67).

As to claim 99, Kirsch discloses a method for the transfer of secure data on a network including the steps of:

a client (12 fig.1) making a request from a server (16 fig.1 and said server retrieving conforming client data (see fig.1, col.5 line 52 to col.6 line 48).

said server creating at least one secure cookie, each of said at least one secure cookie including selected conforming client data, said selected conforming data including at least some of said conforming client data (i.e., using the server to create and to store a client side cookie for use in connection with a subsequent URL request, see figs.1, 2, abstract, col.5 line 53 to col.6 line 49 and col.7 line 43 to col.8 line 52).

said server (16 fig.1) transmitting at least one of said at least one secure cookie to said client and said client storing at least one of said at least one secure cookie (see col.7 line 20 to col.8 line 20).

said client (12 fig.1) presenting to a related server at least one of said stored at least one secure cookie with a second request, said related server residing on the same domain as said server (i.e., cookie having a match of domain, see fig.3, col.11 lines 15-38).

said related server (16 fig.1) making a determination of whether at least one of said at least one retrieved stored at least one secure cookie contains said selected conforming client data and said related server fulfilling said second request if said determination is positive (authenticating the client user to server, see col.9 lines 4-63 and col.14 lines 1-43).

Kirsch does not specifically disclose another cookie in the secure data processing. However, Gupta discloses a cookie containing an encrypt session key capable of encrypting said vale data contained in another of at least one secure cookie (cookie that can that encrypt/decrypt a message, see col.12 lines 7-61 and col.13 line 41 to col.14 line 45). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Gupta's teachings into the computer system of Kirsch to process secure data information because it would have enabled servers to authenticate/process users by implementing users' cookies or tokens in a communications network.

As to claims 100 and 113, Kirsch discloses said conforming client data in retrieved from said client and determination is positive only if said selected conforming client data was retrieved by said server from said client during the current session (verifying a valid user account, col.8 lines 13-63 and col.13 lines 15-67).

As to claim 118, Kirsch discloses a request is part of an attribute-based access control function session (see controlling purchase transactions, see col.14 lines 1-65).
As to claim 79, Kirsch discloses a system for transfer of secure data on a network (internet 14 fig.1) comprising:

a) a client (12 fig.1) capable of presenting conforming client data.

b) a server (server 16 fig.1) capable of using said conforming client data to create at least one secure cookie (i.e., using the server to create and to store a client side cookie for use in connection with a subsequent URL request, see figs.1, 2, abstract, col.5 line 53 to col.6 line 49 and col.7 line 43 to col.8 line 52), at least one secure cookie including:

i) a domain field capable of holding domain data to associate said secure cookie to a domain where said secure cookie is valid (i.e., cookie having a match of domain, see fig.3, col.11 lines 15-38).

ii) at least one name field capable of holding name data (see col.11 lines 15-38).

iii) at least one value field capable of holding value data derived from said conforming client data (see col.11 line 39 to col.12 line 16).

iv) an expiration field capable of holding cookie expiration data (expiration date, col.13 lines 15-67).

c) a network (processing information over a network) capable of transporting at least one secure cookie between said server and said client (see fig.4, 14 lines 1-43).

d) a client storage (cookies stored by client) means capable of storing at least one of said at least one secure cookie and a secure attribute service between said client and said server using said at least one secure cookie (see col.13 line 15 to col.14 line 65).

Kirsch does not specifically disclose another cookie in the secure data processing. However, Gupta discloses a seal cookie used by a server to determine if at least one secure cookie has been altered (see col.12 lines 7-61 and col.13 line 41 to col.14 line 45). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Gupta's teachings into the computer system of Kirsch to process secure data information because it would have enabled servers to authenticate/process users by implementing users' cookies or tokens in a communications network.

As to claim 119, Kirsch discloses at least one of the cookies is an authentication cookie (using authentication mechanism, see col.13 lines 15-67 and col.14 lines 1-65).

As to claim 120, Kirsch discloses a system for transfer of secure data on a network (internet 14 fig.1) comprising:

a) a client (12 fig.1) making request from a server (server 16 fig.1).

b) said sever retrieving conforming client data to create at least one secure cookie (i.e., using the server to create and to store a client side cookie for use in connection with a subsequent URL request, see figs.1, 2, abstract, col.5 line 53 to col.6 line 49 and col.7 line 43 to col.8 line 52), at least one secure cookie including:

i) a domain field capable of holding domain data to associate said secure cookie to a domain where said secure cookie is valid (i.e., cookie having a match of domain, see fig.3, col.11 lines 15-38).

ii) at least one name field capable of holding name data (see col.11 lines 15-38).

iii) at least one value field capable of holding value data derived from said conforming client data (see col.11 line 39 to col.12 line 16).

iv) an expiration field capable of holding cookie expiration data (expiration date, col.13 lines 15-67).

c) a network (processing information over a network) capable of transporting at least one secure cookie between said server and said client (see fig.4, 14 lines 1-43).

d) a client storage (cookies stored by client) means capable of storing at least one of said at least one secure cookie and a secure attribute service between

said client and said server using said at least one secure cookie (see col.13 line 15 to col.14 line 65).

Kirsch does not specifically disclose another cookie in the secure data processing. However, Gupta discloses a seal cookie used by a server to determine if at least one secure cookie has been altered (see col.12 lines 7-61 and col.13 line 41 to col.14 line 45). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Gupta's teachings into the computer system of Kirsch to process secure data information because it would have enabled servers to authenticate/process users by implementing users' cookies or tokens in a communications network.

As to claim 121, Kirsch discloses at least one of the cookies is an authentication cookie (using authentication mechanism, see col.13 lines 15-67 and col.14 lines 1-65).

4. Claims 83-88, 90, 92- 95, 101, 102, 104-108, 109-111 and 114 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kirsch and Gupta as in item 3 above and further in view of Wiser et al US pat. No.6,385,596.

As to claims 83-88, 101, 102, 104, 108, 111 and 114, Kirsch and Gupta's teachings still applied as in item 3 above. Kirsch discloses an encryption algorithm, password cookie including a password (i.e., using encrypting mechanism for cookies, see col.13 lines 15-67). Neither Kirsch nor Gupta specifically disclose the client's IP address, a hashing algorithm, and a digital signature on a timestamp, secret-key based authentication

service. However, Wiser discloses the client's IP address, a hashing algorithm, secret-key based authentication service and an encryption session key (i.e., using multiple levels of encryptions such as Password Authentication Protocol, see abstract, col.16 line 4 to col.19 line 59, col.10 line 13 to col.12 line 54 and col.16 line 4 to col.19 line 59 and col.20 line 10 to col.21 line 61). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Wiser's teachings into the computer system of Kirsch to identify a host computer because it would have enabled users to identify a host connected to the Internet to other Internet hosts and provided more secure delivery of data over the Internet.

As to claim 90, Kirsch discloses at least one secure cookie includes a multitude of secure cookies (see col.13 line 15 to col.14 line 65).

As to claims 92, 93 and 109, Kirsch discloses that the seal cookie includes an integrity check value and the signature of a message digest signed using a private key (see col.8 lines 13-63 and col.13 line 15 to col.14 line 65).

As to claims 94 and 95, Kirsch discloses at least one of said at least one name field and at least one of said at least one value field are a pair, and one secure cookie further includes a flag, said flag specifying whether all machines within said domain referenced by said domain data can access said value data (i.e., information of a cookie including NAME and VALUE, see fig.3, col.11 line 16 to col.12 line 67 and col.13 lines 15-51).

As to claims 105 –107 and 110, Kirsch discloses determination further includes verifying that digital signature belongs to said client and including the step of said server encrypting at least some of said selected conforming client data, a public key and a secret key encrypting a cookie, see col.13 line 1 to col.14 line 65).

5. Claims 89 and 103 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kirsch, Gupta and Wiser as in item 4 above and further in view of Shi et al., US pat. No.5,875,296.

As to claims 89 and 103, Kirsch, Gupta and Wiser's teachings still applied as in item 4 above. Neither Kirsch nor Wiser not Gupta discloses a Kerberos ticket. However, Shi further discloses a Kerberos ticket (see col.5 line 40 to col.6 line 12). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Shi' Kerberos ticket in the computer system of Kirsch to process transactions in the Internet because it would have enabled the functionality of existing standalone Web servers to be enhanced in the enterprise environment and allowed users to easily access the Web information stored in the Distributed File Service namespace with no additional software on the client machine (see Shi's col.2 lines 38-59).

Response to Arguments

6. Applicant's arguments with respect to claims 79, 80, 82-90, 92-95 and 97-121 (filed on 9/13/2004) have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

7. Claims 79, 80, 82-90, 92-95 and 97-121 are ***rejected.***

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khanh Dinh whose telephone number is (571) 272-

3936. The examiner can normally be reached on Monday through Friday from 8:00 A.m. to 5:00 P.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung, can be reached on (703) 272-3939. The fax phone number for this group is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIRI system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Khanh Dinh
Patent Examiner
Art Unit 2151
4/2/2005

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER